ABSTRACT

One aspect of an embodiment of the invention provides a method and platform to prove to a challenger that a responder device possesses cryptographic information from a certifying manufacturer. This is accomplished by performing a direct proof by the responder device to prove that the responder device possesses the cryptographic information. The direct proof comprises at least one exponentiation being conducted using an exponent having a bit length no more than one-half a bit length of a modulus (n).